EXHIBIT A

University of Colorado

Boulder | Colorado Springs | Denver | Anschutz Medical Campus

About the CU System News & Information Students Alumni & Friends Faculty & Staff System Departments

Support CU

About the Accellion Cyberattack

The University of Colorado experienced a cyberattack on a vulnerability in software provided by third-party vendor Accellion, which alerted the university in late January. CU is one of fewer than 50 Accellion customers that were affected by the attack. We believe personally identifiable information from students, employees and others may have been compromised.

CU uses a product called File Transfer Appliance (FTA) from Accellion to provide a large file transfer service used primarily by faculty, staff and researchers. The service is used primarily by the Boulder campus, although some data from the Denver campus was involved as well. System and campus information security teams are working to determine the extent of the attack and the precise nature of the data affected. This page provides information about the incident, what you can do to protect your data and the university's next steps.

The information on this page was last updated: Friday, Feb. 12, 2021.

About the cyberattack

Accellion discovered an attacker was taking advantage of a vulnerability in its large file transfer software (FTA) and notified its clients. CU Boulder's Office of Information Technology (OIT) suspended use of the service on Jan. 25, 2021 and issued a notice to users. The service was restored on Jan. 28, 2021, after a patch was made available by Accellion and files and workspaces were successfully transferred to a new virtual appliance with the newly released version of the software.

A forensic investigation, led by the university's Office of Information Security (OIS) with the assistance of Accellion, revealed CU Boulder's service was compromised and the files available on the system during the attack had been at risk of unauthorized access.

What the University of Colorado is doing

On Monday, Feb. 1, 2021, OIT emailed the 447 CU users that had files uploaded in the large file transfer system in January. As part of the forensic investigation, users were asked to contact the Office of Information Security if they shared highly confidential data during the January timeframe.

OIS continues to conduct a manual review of all files that were exposed to unauthorized access. While the team is continually working on this, manual review can take some time. While we will have a sense of the extent of the attack by the end of this week, a complete investigation will take longer. The goal of this systematic and diligent review is to identify the types of data in these files so that we may work with all affected parties on next steps. Updates will be provided on this page as more details are confirmed regarding exposed data and affected parties.

What kind of data were compromised

While the full scope has not yet been determined, early information from the forensic investigation confirms that the vulnerability was exploited and multiple data types may have been accessed, including CU Boulder and CU Denver student personally identifiable information, prospective student personally identifiable information, employee personally identifiable information, limited health and clinical data, and study and research data.

At this point, data from CU Anschutz, UCCS and system administration does not appear to have been compromised, but the analysis is ongoing.

The results of the forensic investigation will provide information on the exposed data and allow us to provide affected parties with appropriate notification and offer remedies, where necessary.

What to do if you are concerned you are affected

All affected individuals will be notified in a timely manner as the investigation proceeds. Due to the nature of this service and its primary use by CU data custodians, individuals are unlikely at this time to know whether their personal data were impacted. To take proactive steps to protect your identity, learn more about actions you can take at https://www.identitytheft.gov/databreach.

Monitoring services will be made available at no cost for individuals whose confidentiality was compromised. These services detect identity fraud and credit fraud, along with restoration services to address any issues that arise. More information about these services will be provided in the notification letters sent to affected individuals.

Some additional resources to help protect yourself:

Fraud Alerts

- https://www.equifax.com/personal/
- https://www.transunion.com
- https://www.experian.com/

You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freezes

You have the ability to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.

Other Resources

- Information about handling potential identity theft.

Other information

About Accellion File Transfer Appliance

The Large File Transfer service provided by OIT uses a software from Accellion called the FTA, or File Transfer Appliance. It is a solution OIT put in place to provide a mechanism for university faculty and staff to share large files, in lieu of sending them over email. It also provides a secure mechanism for sharing files, meeting the requirements for safe sharing of data required by HIPAA and FERPA. More benefits can be found here: https://oit.colorado.edu/services/file-transfer-storage-infrastructure/large-file-transfer

Upcoming changes to file sharing

OIT is accelerating plans to move to a different file sharing product, which was not affected by this vulnerability. Two additional projects are underway to provide more robust file sharing and account security options for campus. One will migrate on-premises data to hosted cloud solutions and another will deliver a campus-supported multi-factor authentication solution.

Law enforcement and regulatory agencies

Pertinent law enforcement organizations (including the FBI) and appropriate state and federal regulatory agencies have been notified based on the information we have at this time.

Contact Information

CU Boulder
IT Service Center

oithelp@colorado.edu
303-735-4357

CU Denver
Lynx Central

lynx.central@ucdenver.edu
303-315-5969

What is the CU System?
CU Boulder
CU Colorado Springs
CU Denver
CU Anschutz Medical Campus

CU News and Information
Media Contacts
News Releases
Open Records Requests
Contact Us

CU Careers
CU Connections Newsletter
Employee Services (HR, Benefits, Payroll)
Procurement Service Center

CU For Colorado Outreach
CU Facts and Figures
Accountability Data Center
CU Online

1800 Grant Street, Suite 800 | Denver, CO 80203
General: (303) 860-5600 | Fax: (303) 860-5610 | Media: (303) 860-5626